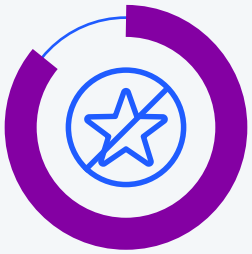
telesign | PNC BANK

PNC Bank, do you know the person behind the number?

eBook

What is more personal than personal identity, PNC Bank?

Victims of identity theft often experience emotions similar to losing a loved one: anger, anxiety, and helplessness. In addition, victims of identity fraud lose confidence in the financial institutions they feel did not adequately protect them, often assigning their anger directly to the company instead of the fraudster. In fact, a recent study shows that 85% of customers would avoid using a brand after losing trust.



85%
of consumers
would avoid using a brand after losing trust.

Building and analyzing digital identity

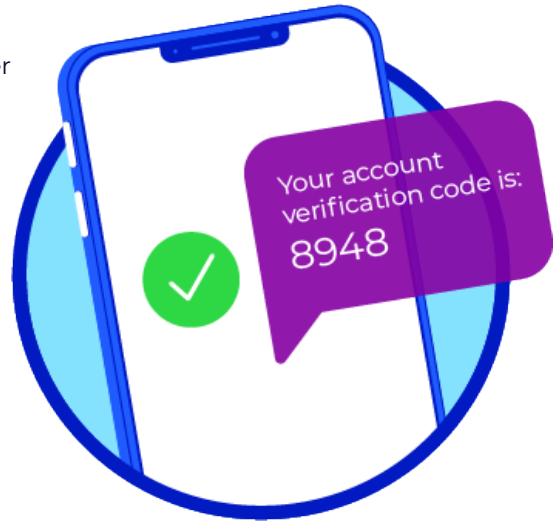
Today, customers expect you to keep them and their digital transactions safe. To do so, you must ensure the users who enter and interact in your ecosystem are who they say they are—at every touchpoint, every time.

In face-to-face transactions, such as withdrawing money from a local bank, identity and verification happens quickly with government-issued identification and proof of address. If the face and signature on the card match the person providing it, the transaction can safely occur.

In the digital world, differentiating between real and fraudulent users attempting to access your ecosystem is more complex, making it critical to establish a consistent and evolving process to build a trusted identity for each user.

Using multifactor authentication as baseline fraud prevention

Customers expect to provide a variety of personal information when creating an online account, including a username, email, password, and other identifying information. Though necessary, a username and password are no longer enough to verify identity and maintain account integrity. The next step in building and verifying a digital identity is multifactor authentication (MFA).



Multifactor authentication provides a critical, foundational step to protecting your ecosystem and keeping your customers' trust. From global fintech players to your local credit union, MFA has become a user expectation when creating accounts and protecting transactions.

MFA remains a solid defense against stolen passwords, but MFA doesn't comprehensively verify the person behind the phone number. When customers receive a one-time passcode (OTP) to verify their identity, it ensures they have access to the mobile phone number listed, but fraudsters continue to challenge the limitations of MFA.

Who is the person behind the phone number?

Bad actors have moved beyond stealing passwords to taking over accounts and identities. Today's fraudsters gather details from various sources to assume a victim's identity or create an entirely new synthetic identity. They purchase stolen emails, passwords, and numbers on the dark web, utilize sophisticated malware and social engineering scams, find answers to knowledge-based identifiers from social media postings, and more. If the data is out there, fraudsters will find it and use it in their schemes.

Although MFA remains essential, fraudsters learn and adapt, which means that financial organizations must do the same to remain secure. Fraudsters have found ways around MFA security measures by exploiting unencrypted burner phones in SIM farms, deploying batches of VoIP numbers, conducting social engineering and SIM swap attacks, and developing and implementing other constantly evolving fraud techniques and practices. Traditional MFA lacks a digital identification and risk assessment to determine the legitimacy of the person behind the phone number.

Hidden behind the scenes, phone numbers hold critical insights about the end-user. These identity and behavioral signals offer a complete snapshot of the person attempting to enter and transact in your ecosystem.

To decrease friction for your good users while making life more difficult for fraudsters, the best approach to preventing fraud is to use the phone number provided for MFA to gain deeper identity insights. With this approach, you can block access for suspicious behavior with minimal friction to your legitimate customers.

A dynamic, risk-based digital identity assessment adds security without adding friction.

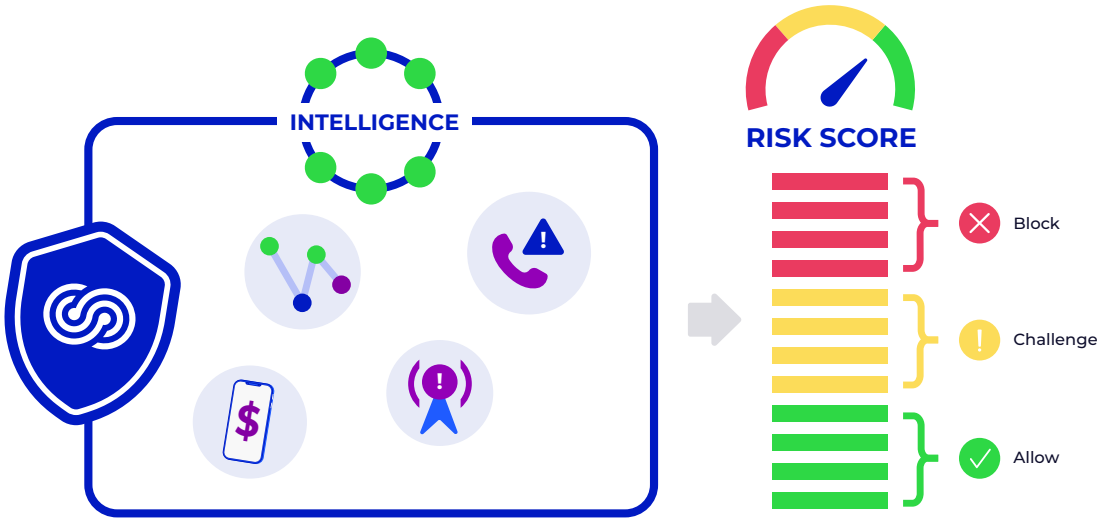
Checking for reputation and risk can be completed in milliseconds, working seamlessly alongside MFA or biometric verification.

Seamless verification and identification

Using Telesign MFA with risk and reputation assessments, businesses around the globe are protecting their ecosystems from bad actors while providing superior customer service to verified customers.

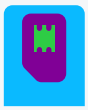
Telesign Intelligence is a dynamic risk assessment that uses machine learning to analyze phone number data and delivers a phone number reputation score.

Intelligence assesses the riskiness of users through phone number attributes and recommends whether to **allow, flag, or block** them based on their risk score. When Intelligence recommends flagging an interaction, you can opt to review the registration or transaction manually. When Intelligence recommends allowing an interaction, the optional next step is to send a one-time passcode that the user then provides to verify their identity or transactional activity.



Certain aspects that Telesign deems risky result in a higher score. What types of behavior would negatively impact a user's score? A VoIP phone number, a burner phone, or a phone number that has recently changed devices (SIM swap) each raises a flag and increases the risk score. Intelligence goes beyond MFA and helps you answer critical security and business questions, such as:

Is this OTP at risk of being intercepted by a bad actor?



Has this phone number been recently SIM swapped, ported out, or forwarded to another phone number?

Is this log-in or password reset a potential account takeover attempt?

Are we wasting money sending an SMS and/or voice call to this number?

Intelligence is natively integrated into Telesign's Verification API and requires minimal developer resources to get started. And when you layer in account takeover attributes, you can build trust at every stage of the customer journey.

There is an emotional impact to identify theft that can have far-reaching effects on your customers and reputation. You do not want that pain associated with your brand. When paired with multifactor authentication, Intelligence is the ultimate gatekeeper for financial platform security and helps keep your customers happy, safe, and coming back.

Saving costs with KYC

For banks and financial institutions, maintaining compliance with know your customer (KYC) regulations is necessary, but can be costly.

Start your KYC program with mobile identity insights. Enterprises can detect fake and fraudulent users as the first step in the KYC process to block bad actors before completing more costly KYC steps like document verification. By leveraging Telesign you can implement low-friction and low-cost solutions to verify a new user's name, address, and silently verify whether their provided mobile number is active as expected. This allows your KYC program to fast-track legitimate users while eliminating wasteful checks for high-risk users.

Ready to deliver a trusted financial experience?

Get started